

Plaintiff, Genesco Inc., a Tennessee corporation, filed this action under 28 U.S.C. § 1332, the federal diversity jurisdiction statute against the Defendants: Visa U.S.A. Inc., Visa Inc., and Visa International Service Association (collectively “Visa”), Delaware corporations with their principal places of business in California. Genesco asserts state law claims against the Visa Defendants arising out of Visa’s assessments of \$13,298,900.16 in non-compliance fines and reimbursement assessments. Visa imposed these assessments against Wells Fargo Bank, N.A. and Fifth Third Financial Corporation under Visa’s agreements with those banks to process retail purchases with Visa credit and debit cards. Wells Fargo and Fifth Third had separate agreements with Genesco to process Visa credit and debit card transactions for purchases at Genesco’s retail establishments. Wells Fargo and Fifth Third also had indemnification agreements with Genesco under which Genesco agreed to indemnify Fifth Third and Wells Fargo for the banks’ losses incurred in processing Visa credit and debit card transactions with Genesco’s retail establishments. Fifth Third and Wells Fargo then collected Visa’s assessments from Genesco.

For this action, Genesco is the assignee and subrogee of Fifth Third and Wells Fargo for any claims of those banks against Visa for these fines and assessments. Genesco asserts multiple claims for Visa's alleged breaches of contracts and implied covenants of good faith and fair dealing in imposing and collecting these fines and reimbursement assessments. Genesco also asserts claims under the California Unfair Competition Act, Cal. Bus & Prof. Code §17200 et seq. and common law claims of unjust enrichment and restitution. The specifics of Genesco's claims are, in essence, that Visa's fines and assessments against the banks lack a factual basis and were imposed in violation of Visa's Visa International Operating Regulations ("VIOR")¹ that are incorporated into Visa's agreements with Wells Fargo and Fifth Third. Genesco seeks recovery of Visa's fines and assessments against the banks as well as incidental damages incurred by these banks and Genesco due to Visa's alleged wrongful conduct in imposing and collecting these fines and assessments.

Before the Court is Visa's motion to dismiss (Docket Entry No. 30) that seeks dismissal of Genesco's sixth and seventh claims under the California Unfair Competition Law ("UCL") and common law claims for unjust enrichment and restitution. In sum, Visa argues: (1) that given the express provisions of Visa's contracts with the banks authorizing the fines and assessments, Genesco cannot rely on such contracts for an actionable claim under the California's UCL; (2) that Genesco has not adequately pled fraud for its claim under the UCL; (3) that restitution is unavailable to Genesco that was not a party to Visa's agreements with the banks under which the fines and assessment were imposed; and (4) that the express provisions of Visa's contracts with the banks preclude Genesco's common law claims for equitable relief.

¹ Neither Visa's VIOR nor its security standards are attached to Genesco's complaint. In addition, the parties agreements cited in the complaint are not attached to the complaint. Genesco's allegations describe the content or quote pertinent provisions of these materials.

In response, Gensco contends, in essence: (1) that Visa's breaches of its contracts with the banks can state claims under the California's UCL; (2) that Genesco has adequately pled fraud for its claim under the UCL; and (3) that restitution is available to Genesco as the funds for the unlawful fines and assessments against the banks are directly traceable to Genesco, the ultimate source of those funds paid to Visa.

In its reply, Visa reasserts that under California law, the express provisions of its contracts with the banks authorizing these fines and assessments are not actionable under California's UCL and Genesco cannot invoke equitable claims to alter those contract terms.

For the reasons set forth below, the Court concludes that decisions under California's UCL, recognize claims based upon contracts of commercial entities where breaches of such contract violate public policy or harm competition or consumers. Here, Genesco asserts claims that Visa's fines and assessments against the banks that Genesco actually paid, lacked a factual basis and were contrary to Visa's agreements with the banks and were contrary to the forensic evidence about the effects of the cyber attack on Genesco's computer system. Genesco asserts that these fines are also penalties that are unenforceable as a matter of California law. Violations of California law can state a claim under California law. Moreover, Visa's alleged imposition of more than \$13 million dollars in fines and assessments, without a factual basis and in violation of Visa's standards, impacts retail transactions involving consumers, retail merchants and other banks and implicate fairness in the credit and debit card markets. Thus, the Court concludes that Genesco's UCL and common claims under California law are actionable.

A. Analysis of the Complaint

1. The Parties

Genesco sells footwear, headwear, sports apparel and accessories at its more than 2,440 retail stores throughout the United States, Canada, the United Kingdom and the Republic of Ireland. (Docket Entry No.1, Complaint at ¶ 2). Genesco's products bear the trade names: Journeys, Journeys Kidz, Shi by Journeys, Underground by Journeys, Schuh, Lids, Lids Locker Room and Johnston & Murphy. Genesco also sells from its internet websites. Id.

Visa Inc. operates an international payment system for its credit and debit cards under contracts with financial institutions that enable those financial institutions' customers, cardholders and merchants, to pay for and receive payments for transactions utilizing Visa credit and debit cards. Id. at ¶ 3. Visa USA, Visa's principal subsidiary in the United States, operates a retail electronic payments network to facilitate payments to financial institutions and businesses for consumer purchases. Id. at ¶ 4. Visa International operates a global processing platform that services payment transactions throughout the world. Id. at ¶ 5

Financial institutions in the Visa system enter into a license agreement as "issuers" and/or "acquirers" of Visa credit and/or debit cards. Id. at ¶ 9. Visa issuers contract with their cardholders for their use of Visa-branded cards to purchase goods or services in the marketplace. A Visa "acquirer" contracts with merchants to accept and process payments with Visa cards. Id. The Visa network has a daily funds flow that pays the participating merchants for Visa-branded transactions. Id. The Visa acquirer collects that amount from Visa and Visa then collects from the relevant Visa issuers. Id. The Visa issuers collect the amounts paid from the individual Visa cardholders who made the purchases with the participating merchant. Id.

Here, Wells Fargo was Genesco's Visa acquirer for Visa transactions at Genesco's retail establishments with Visa credit card and non-PIN debit card transactions. Id. at ¶ 10. Fifth Third Bank was Genesco's acquirer for Visa PIN debit card transactions. Id. For its agreements with Fifth Third and Wells Fargo, Genesco agreed to pay Wells Fargo and Fifth Third a "interchange fee" that is a percentage of the dollar value of each transaction with a Visa card. Id. at ¶ 11. These banks retain a share of these fees and the balance of these fees are paid to Visa. Id. In turn, Visa retains a portion of these fees and the remaining fees are paid to other financial institutions that were parties to the transactions. Id. For these transactions, Genesco agrees to comply with the VIOR as applicable to merchants. Visa's VIOR includes Payment Card Industry Data Security Standards ("PCIDS") that set forth security standards developed by firms, including Visa, that create and operate in the credit and debit card market for issuing and acquiring banks as well as merchants. Id. at ¶ 15. The PCIDS applies to all system components of any entity subject to the PCIDS. Id. at ¶ 16. Genesco's agreement with Fifth Third includes the following indemnification provisions:

Notwithstanding any other provision of this Agreement, Merchant shall be responsible for all fees, assessments and penalties imposed by third party providers such as, but not limited to, VISA, MasterCard, Other networks and telecommunication companies, and any changes or increases shall automatically become effective without notice and shall be immediately payable by [Genesco] when assessed by [Fifth Third].

Id. at ¶ 13. (quoting Fifth Third Agreement at Section 13).

Genesco's agreement with Wells Fargo also contains indemnification provisions: "You agree to pay any fines imposed on us by any Association resulting from Chargebacks and any other fees or fines imposed by an Association with respect to your acts or omissions" and "You agree to indemnify and hold us harmless from and against all losses, liabilities, damages and expenses . . .

arising out of any third party indemnifications we are obligated to make as a result of your actions (including indemnification of any Association or Issuer).” Id. at ¶ 14. (quoting Wells Fargo Agreement at Sections 18.9, 26.1.d).

On April 21, 2011, Genesco, Wells Fargo, and Wells Fargo Merchant Services, L.L.C. also entered into a Reserve Agreement under which Genesco funded a reserve account for potential fines, issuer fraud and operating expense assessments and/or other assessments that could be imposed upon Wells Fargo by Visa under the VIOR. Id. at ¶ 36. In this Reserve Agreement, Genesco acknowledged its obligation to indemnify Wells Fargo for the amount of any such assessments, regardless of whether the assessment was valid under the VIOR or under applicable law. Id. at ¶ 37. In turn, Wells Fargo agreed that upon reimbursement by Genesco for any such fine or assessment from the reserve account or otherwise, Wells Fargo would assign, transfer and convey to Genesco any and all rights or claims that Wells Fargo may have against Visa to obtain reimbursement of any portion of such fine or assessment. Id. at ¶ 38. In sum, Genesco was fully subrogated to any and all such rights or claims.

2. Cyber Attack on Genesco's Computer Network

From December 2009 to December 2010, computer hackers accessed Genesco’s computer network by compromising a particular feature of security protocols that govern payment of card transactions in the United States. Id. at ¶ 17. Most payment card transactions are initiated by the account holder’s payment card being “swiped” at the point of sale. Each Visa card has a “mag-stripe” with the necessary information to effect the purchase, including the account number, the card’s expiration date, and the card’s CVC, a security code. Id. at ¶ 18. The merchant swipes the customer’s Visa card and the card’s mag-stripe’s information is electronically transmitted to the

merchant's acquiring bank and then to the cardholder's issuing bank. Id. These transactions are referred to as a "mag-stripe-swipe transaction." Id.

The cyber attackers stole payment card account data as Genesco transmitted that data to Fifth Third and Wells Fargo in unencrypted form during the approval process. Id. at ¶¶ 19, 20. To do so, the cyber attackers inserted into Genesco's computer network malicious software ("malware") that employs a "packet sniffer" technology to acquire unencrypted account data in transit through Genesco's computer network's transmissions to Fifth Third or Wells Fargo for transaction approval. Id. The cyber attackers, however, did not access any stored payment card account information in Genesco's computer network. Id. at ¶ 21

Upon discovery of this cyber attack on Genesco's computer data, Visa issued a Compromise Account Management Systems Alert ("CAMS Alert") to its issuers for every Visa account that Genesco processed through Genesco's cardholder data environment from December 4, 2009 through December 1, 2010. Id. at ¶ 22. Genesco alleges that the forensic evidence reflects that none of the Alerted Accounts in the Genesco transactions has been compromised by this cyber attack and that the forensic evidence "affirmatively showed" that some Alerted Accounts were not compromised by the cyber attack on Genesco's computer system. Id.

3. Visa's Fines and Assessments

By letters dated May 31, 2011, Visa notified Wells Fargo and Fifth Third that in light of the Genesco cyber attack, as Acquiring Banks, each bank was non-compliant with the PCI DSS and the VIOR's Cardholder Information Security Program ("CISP") and assessed each a fine of \$5,000 (the "Non-Compliance Fines"). Id. at ¶¶ 39. Visa's notices also stated that the fines were imposed under ID# 041010-41010-0008031 of the VIOR, and that the amount of the fines were calculated under

ID# 021010- 041010-0009032 of the VIOR. Id. at ¶ 46. These notices also informed Fifth Third and Wells Fargo that under ID#: 010410-010410-0007289 of the VIOR, each had 30 days from the receipt of the notices to appeal the fines to Visa. Id. On or about June 17, 2011, Visa collected \$5,000 from each of the Acquiring Banks in Non-Compliance Fines. Id. at ¶ 42. By a June 30, 2011 letter, Fifth Third appealed its fine, and by letter dated July 6, 2011, Wells Fargo appealed its fine. Id. at ¶ 47. Genesco alleges that Visa has not ruled on either appeal, but retains the \$10,000 in fines that were collected in 2011. Id. Under its reserve agreement with Genesco, Wells Fargo then transferred \$5,000 from Genesco's reserve account as reimbursement for that fine. Id. at ¶ 42. Similarly, Fifth Third withheld \$5,000 from settlement funds otherwise due to Genesco as reimbursement for its fine as authorized by its agreement with Genesco. Id.

In a November 8, 2011 letter, Visa notified Wells Fargo and Fifth Third of Visa's determination that the Genesco cyber attack qualified for the ADCR process under which Visa calculated the liability of Wells Fargo and Fifth Third and assessed the banks for \$5,167,714.58 (the "ADCR Assessment"), with \$2,773,536.00 attributed to the "Operating Expense Recovery Assessment") and \$2,394,178.58 attributed to the Counterfeit Fraud Recovery. Id. at ¶ 40. In a separate November 8, 2011 letter, Visa notified Wells Fargo that the Genesco cyber attack also qualified for the DCRS process and had assessed DCRS liability against Wells Fargo in the amount of \$8,121,185.58 (the "DCRS Assessment"). Id. at ¶ 41.

On or about January 5, 2013, Visa collected these assessments from Wells Fargo arising out of the Genesco cyber attack by withholding \$11,996,66 in Visa payments otherwise owed to Wells Fargo. Id. at ¶ 43. This total included \$2,301,693.53 in Counterfeit Fraud Recovery; \$1,573,785.60 in Operating Expense Recovery, and the \$8,121,185.58 in DCRS Assessments under Wells Fargo

Assessments agreement. Id. Wells Fargo then transferred \$11,996,664.71 from Genesco's indemnification and reserve account agreements as reimbursement for these Visa assessments under Genesco's reserve agreement with Wells Fargo. On or about January 5, 2013, by a similar withholding, Visa collected \$1,342,409.93 from Fifth Third representing: \$142,659.53 in Counterfeit Fraud Recovery and \$1,199,750.40 in Operating Expense Recovery under Fifth Third's agreement with Visa. Id. at ¶ 44. In turn, Fifth Third then withheld \$1,342,409.93 from Genesco's indemnification agreement as reimbursement for these assessments. Id.

Genesco alleges that in calculating these amounts, Visa found certain Alerted-Accounts ineligible for the ADCR and DCRS processes despite their inclusion in the CAMS Alerts that Visa issued on the cyber attacks on Genesco's system. Id. at ¶ 45. Genesco further alleges that the forensic evidence showed that these accounts had not been compromised during the cyber attack, but Visa nonetheless deemed those Alerted-On Accounts eligible for the ADCR and DCRS assessments. Id. Genesco alleges that at some point, Visa found other Alerted-Accounts eligible for the ADCR and DCRS assessments despite the lack of forensic evidence that these accounts were compromised during the cyber attacks on Genesco's computer system. Id. at ¶ 46.

4. Visa's Data Security Standards for Payments

According to Genesco, Visa's VIOR requires all acquiring banks to require their merchants to comply with VIOR's PCIDSS. Id. at ¶ 15 (citing VIOR ID#: 081010-010410-0003356). The PCI DSS sets forth data security requirements developed by the card brands in this market, including Visa, through those firms' Payment Card Industry Security Standards Council. Id. The PCI DSS is described as theft protection of payment card account data (including account number, the expiration date, and the card verification codes that are embedded in the card's magnetic stripe and printed on

the back of the card). Id. These standards are to prevent, during the merchant transactions, theft of such data that can be used to manufacture counterfeit cards for fraudulent transactions on the compromised card account. Id. PCI DSS's "system components" include a network component, server, or application that is part of the "cardholder data environment." Id. at ¶ 16. This "cardholder data environment is comprised of people, processes and technology that store, process or transmit cardholder data or sensitive authentication data on behalf of an entity." Id. Under the PCI DSS, any firm in this environment may employ network segmentation to limit the "system components" within that firm's network, but such systems remain subject to the PCI DSS. Id.

Genesco alleges that cyber attacks focus on the payment card system's unencrypted data during the credit or debit card's mag-stripe-swipe transaction. According to Genesco, Visa's VIOR's PCI DSS permits the payment card account data required for approval of a mag-stripe-swipe transaction, to be unencrypted during the transaction approval process. Id. at ¶ 19. For cyber attackers, this unencrypted payment card data is sought to create a counterfeit card through which fraudulent transactions on that account can occur. Genesco also alleges that the VIOR does not prohibit retention of unencrypted data in the mag-stripe-swipe transaction during the authorization process for a transaction. Id. (citing VIOR ID#: 081010-010410-0002228).

5. Visa's Recovery Processes

In the event a merchant's network is compromised by a cyber attack, Visa's VIOR has two processes to impose liability upon the affected acquiring bank for losses incurred by Visa issuers: the Account Data Compromise Recovery ("ADCR") and the Data Compromise Recovery Solution ("DCRS") processes. Id. at ¶ 23. According to Genesco, Visa considers the ADCR to provide an agreed mechanism to determine (1) whether the data security breach in question resulted in an

“account compromise event” of Visa card for any particular Visa account issued in the United States and (2) whether the merchant or its acquirer is responsible for the breach. Id. at ¶ 24. In addition, the ADCR authorizes the determination of counterfeit fraud losses and operating expenses that any U.S. Visa issuers incurred due to the security breach and during Visa’s collection of the contractually specified losses from the Visa acquirer in question. Id.

A Visa acquirer’s potential liability under the ADCR Recovery process includes Counterfeit Fraud Recovery and Operating Expense Recovery. Id. at ¶ 25. The Counterfeit Fraud Recovery applies to losses attributable to any counterfeit fraud losses from compromises of Visa’s magnetic-stripe-data account of the acquiring bank’s merchant(s). Id. Genesco alleges that under the VIOR, Counterfeit Fraud Recovery arises only when: (1) the “account compromise event” involves the full contents of the card’s magnetic stripe for at least 10,000 particular U.S.-issued Visa accounts; (2) a CAMS Alert for the compromised Visa accounts was issued to the issuers of those Visa accounts; (3) “incremental fraud” occurs that is attributable to the compromised Visa accounts; and (4) the merchant in question has committed at least one of the following PCI DSS violations:

- (a) stored the full contents of any track on the magnetic stripe after authorization of a transaction and such retention allowed the compromise of the full contents of any track on the magnetic stripe of the compromised Visa accounts,
- (b) committed some other violation of the PCI DSS that could have allowed the compromise of the full contents of any track on the magnetic stripe of the particular Visa accounts that suffered the account compromise event, or
- (c) committed a violation of the PIN Management Requirements Documents that could have allowed a compromise of PIN data of the compromised Visa accounts after authorization of transactions on those accounts.

Id.

Genesco alleges that Visa’s VIOR does not define an “account compromise event,” but Visa

allegedly interprets an “account compromise event” for any particular Visa account “as an actual theft of cardholder data relative to that account (as opposed to the mere possibility of such theft).” Id. at ¶ 26. According to Genesco, the only reasonable or most reasonable interpretation of “account compromise event” for any compromised Visa account is “actual theft of cardholder data relative to that account (as opposed to the mere possibility of such theft).” Id.

Visa’s VIOR defines “incremental fraud” for ADCR, as the portion (if any) of reported counterfeit fraud on a compromised U.S. issued Visa account that suffered a loss above the “baseline counterfeit fraud level” for those accounts for the particular period of the compromise. Id. at ¶ 27. Visa’s VIOR does not define “baseline counterfeit fraud level,” but for ADCR purposes, Visa allegedly interprets that term as “the amount of counterfeit fraud that normally would have been expected to have been reported on the accounts in question for the period in question, taking into account the rampant counterfeit fraud that any particular account, or group of accounts, in the Visa system is subject to at any given point in time.” Genesco alleges that the only reasonable or most reasonable interpretation of “baseline counterfeit fraud level” for ADCR purposes is the amount of counterfeit fraud that normally would have been expected to have been reported on the accounts in question for the period in question. Id.

For a Visa acquiring bank, Visa’s VIOR does not impose liability upon a Visa acquirer for Counterfeit Fraud Recovery involving the activities of one of its merchants unless: (1) the merchant suffered a theft of cardholder data for not less than 10,000 particular U.S.-issued Visa accounts, (2) the merchant committed a PCI DSS violation that allowed (or at a minimum could have allowed) the theft to occur, and (3) the compromised Visa accounts thereafter incurred an amount of counterfeit fraud in excess of the amount of counterfeit fraud beyond that normally expected to have

been reported on the accounts in question for the period at issue. Id. at ¶ 28.

For Operating Expense Recovery, a Visa acquirer can be liable to U.S. Visa issuers for a magnetic-stripe-data account compromise event suffered by one of the acquirer's merchants. This liability requires: (1) an account compromise event involving the full contents of any track on the card's magnetic stripe occurs for at least 10,000 particular U.S.-issued Visa accounts; (2) a CAMS Alert for the compromised Visa accounts that was sent to the issuers of those accounts; and (3) the merchant in question committed at least one of the following PCI DSS violations:

- (a) stored the full contents of any track on the magnetic stripe subsequent to authorization of a transaction and thereby allowed the compromise of the full contents of any track on the magnetic stripe of the particular Visa accounts that suffered the account compromise event,

- (b) committed some other violation of the PCI DSS that could have allowed the compromise of the full contents of any track on the magnetic stripe of the particular Visa accounts that suffered the account compromise event, or

- (c) committed a violation of the PIN Management Requirements Documents that could have allowed a compromise of PIN data for a Visa Transaction, a Plus transaction, or an Interlink transaction subsequent to authorization.

Id. at ¶ 29.

Under the VIOR, a Visa acquirer is not liable to Visa for Operating Expense Recovery due to the activities of one of its merchants “unless (1) the merchant suffered a theft of cardholder data with respect to not less than 10,000 particular U.S.-issued Visa accounts, and (2) the merchant committed a PCI DSS violation that allowed (or at a minimum could have allowed) the theft to occur.” Id. at ¶ 30. Moreover, even in that event, Visa’s VIOR provides that a Visa acquirer can be contractual liable to Visa for Operating Expense Recovery for the activities of one of its merchants only if, and only to the extent, operating expenses are “in fact incurred by the issuers of

the Visa accounts in question as a result of the theft in question.” Id.

When a Visa acquirer's merchant suffers a data security breach involving its cardholder data environment, Visa deems its DCRS to authorize a determination of (1) whether the data security breach resulted in a theft of cardholder data relative to any Visa account issued by non-U.S. issuers; (2) whether the merchant in question (and its acquirer) bears responsibility for that theft and; (3) to determine the counterfeit fraud losses of non-U.S. Visa issuers due to that theft. Id. at ¶ 31. Visa collects any losses from the acquiring bank for that Visa merchant. For an acquiring bank's liability to Visa under the DCRS process, the VIOR requires:

- (1) a “data compromise event” involving the theft of full-magnetic stripe data occurs with respect to at least 10,000 particular Visa accounts issued by non-U.S. Visa issuers;
- (2) the data compromise event involves a combined total of \$100,000 or more of full-magnetic stripe counterfeit fraud having occurred during the period in question on the particular Visa accounts that were compromised in the event;
- (3) “incremental fraud” is attributable to the particular Visa accounts that suffered the data compromise event; and
- (4) the merchant in question has committed a violation of the PCI DSS that could have allowed the theft of the full contents of any track on the magnetic stripe of the particular Visa accounts that suffered the data compromise event.

Id. at ¶ 32.

The VIOR does not define the term “data compromise event” for the DCRS, but Visa interprets “data compromise event” as an actual theft of cardholder data relative to a compromised account (as opposed to the mere possibility of such theft).” Id. at ¶ 33. Again, Genesco alleges that the only reasonable or most reasonable interpretation of “data compromise event” for a Visa account for DCRS purposes is “actual theft of cardholder data relative to that account (as opposed to the mere

possibility of such theft).” Id. Visa’s VIOR also fails to define “incremental fraud”, but Visa interprets that term “as the portion (if any) of the counterfeit fraud reported on the particular non-U.S.-issued Visa accounts that suffered the data compromise event in question that is above the amount of counterfeit fraud that normally would have been expected to have been reported on the accounts in question for the period in question, taking into account the rampant counterfeit fraud that any particular account, or group of accounts, in the Visa system is subject to at any given point in time.” Id. at ¶ 34. Genesco asserts that “the only reasonable (or at a minimum the most reasonable) interpretation of ‘incremental fraud’ for the DCRS, is ‘the counterfeit fraud reported on those accounts that is above the amount of counterfeit fraud that normally would have been expected to have been reported on those accounts for the period in question.’” Id.

For a Visa acquirer to be liable under the VIOR for the DCRS process, one of its merchants must have “(1) . . . suffered a theft of cardholder data with respect to not less than 10,000 particular non U.S.-issued Visa accounts, (2) the merchant committed a PCI DSS violation that allowed (or at a minimum could have allowed) the theft to occur, and (3) the compromised group of Visa accounts thereafter incurred an amount of counterfeit fraud in excess of the amount of counterfeit fraud that normally would have been expected to have been reported on the accounts in question for the period in question.” Id. at ¶ 35.

5. Genesco’s Theories of Breach

a. Visa’s Invalid Non-Compliance Fines

Genesco first asserts that Visa’s Non-Compliance Fines imposed on Wells Fargo and Fifth Third violated Visa’s contracts with Fifth Third and Wells Fargo because at the time of cyber attack and at all other relevant times, Genesco was in compliance with the PCI DSS requirements. Id. at

¶ 48. Thus, Genesco contends that neither Fifth Third nor Wells Fargo could have violated their contractual obligations to Visa to require Genesco to maintain compliance with the PCI DSS requirements. Id. Genesco also alleges that Visa lacked a reasonable factual basis to conclude that Genesco was non-compliant with the PCI DSS requirements during the cyber attack or at any other relevant time. Id.

As to these fines, Genesco further asserts that Visa also failed to comply with its VIOR in issuing its notices of noncompliance and enforcing these fines because Visa's VOIR's provisions on "Fines and Penalties Process" sets forth four distinct steps for imposition of a fine:

- (1) Allegation of a violation brought by a Member or Visa officer (ID# 010410-010410-0007366);
- (2) Investigation of the allegations by Visa, including the issuance of a Notification to the Member under investigation (ID# 010410-010410-0007366);
- (3) Determination of a violation, based on the Member's response to the Notification or the Member's failure to respond (ID# 010410-010410-0001052); and
- (4) Notification of Visa's determination that a violation occurred, that a fine is being assessed, and that the Member has a right of appeal (ID# 010410-010410-0001054).

Id. at ¶ 49. According to Genesco, "[e]ach step is dependent on the preceding steps." Id.

The alleged specific violations of these procedures include that the factual bases for these fines were not predicated upon Visa member's or Visa officer's allegations, as required by ID# 010410-010410-0007366. Id. at ¶ 50. Further, Genesco alleges the Visa staff never sent a notification to either Fifth Third or Wells Fargo prior to imposing the fines, as required by ID# 010410-010410-0007366. Id. The Visa staff allegedly did not offer nor permit Fifth Third or Wells Fargo the opportunity to respond to allegations that those banks are in fact subject to the non-compliance fines, as required by ID# 010410-010410-0001052. Id. According to Genesco, without a member's response to the notification, Visa lacked a valid basis under the VIOR to impose Non-Compliance Fines, even if Fifth Third and/or Wells Fargo in some respect violated its

obligation to Visa to ensure Genesco's compliance with the PCI DSS requirements. Id. Genesco denies the latter assumption. Id.

Genesco's next theory is that the Non-Compliance Fines are legally unenforceable penalties, as opposed to damages, for an Acquiring Bank's alleged breach of its contracts with Visa. Id. at ¶ 51. This characterization of a penalty is predicated upon the allegations that the amounts do not represent the actual damages Visa incurred by reason of the Acquiring Banks' alleged failures to cause Genesco's alleged noncompliance with PCI DSS requirements. Genesco contends that these fines cannot be liquidated damages because: (1) Visa possesses unbounded discretion under its VIOR to impose Non-Compliance Fines; (2) the amount of the fines lacks any reasonable relationship to any harm to Visa; (3) the alleged facts do not establish any violation of the Acquiring Banks' obligation to cause Genesco to comply with PCI DSS requirements; and (4) these fines are not Visa's exclusive damages remedy for an Acquiring Bank's alleged violations. Id. For these reasons, Genesco contends that Visa's NonCompliance Fines are invalid and unenforceable alone or in combination with Visa's Counterfeit Fraud Recovery Assessments. Id.

b. Visa's Counterfeit Fraud Recovery Assessments

For its challenges to Visa's Counterfeit Fraud Recovery Assessments against Wells Fargo and Fifth Third, Genesco first asserts that Visa did not establish a factual basis that Genesco suffered a theft of cardholder data for all the U.S.-issued Alerted-Accounts that Visa deemed eligible for these ADCR assessment. Id. at ¶ 51. Second, Genesco contends that Visa's charge that Genesco committed a PCI DSS violation that allowed the theft of cardholder data for all U.S.-issued Alerted-Accounts that Visa considered eligible for ADCR assessments, is baseless. Id. Third, Genesco asserts that Visa's determination of the amount of counterfeit fraud involved, was in excess

of the amount of counterfeit fraud that normally would have been expected to have been reported for the accounts and time period at issue. Id.

Genesco's related claim has several subparts. In this regard, Genesco contends that to be eligible for counterfeit fraud for the ADCR assessment, Visa's VIOR requires an "account compromise event." Id. at ¶ 53. The term "account compromise event" means "actual theft of cardholder data relative to the account in question." Id. According to Genesco, Visa did not establish and cannot show that Genesco suffered an actual theft of cardholder data for all the U.S.-issued Alerted-Accounts that Visa found to be eligible for the ADCR process. According to Genesco, for some U.S.-issued Alerted-Accounts that Visa found eligible for the ADCR process, forensic evidence affirmatively showed that those accounts had not been compromised during the cyber attack on Genesco's computer system. Id. For other Visa accounts that Visa found to be eligible for the ADCR process, Genesco cites the lack of any forensic evidence that those accounts had been compromised as the result of the cyber attack on Genesco's computer. Id.

Genesco's next theory of Visa's breach of its agreements with the banks is ambiguous to the Court. Genesco appears to allege that the cyber attackers' compromise of Genesco's data system caused Genesco's computer system to reboot and thereby precluded any access to Visa account data on Genesco's system. Id. at ¶ 54. Without such access, Genesco challenges Visa's ADCR assessments as lacking a factual predicate. This paragraph is quoted in its entirety:

Moreover, in further regard to Paragraph 52(1) above, certain of the U.S.-issued Alerted-On Accounts on which the Counterfeit Fraud Recovery Assessment is based could not even possibly have suffered an account compromise event during the course of the Intrusion, because reboots of the intruded-upon servers in the Genesco cardholder data environment caused any log files that may have contained data relative to those accounts to be overwritten by the intruder(s)' malware prior to the intruder(s)' having an opportunity to exfiltrate those files from Genesco's network.

Thus, even if the term "account compromise event" as used in the ADCR means merely a possible theft of cardholder data relative to the account in question, and not an actual theft of such data (which is not the case), as a result of such overwriting Genesco did not even suffer a possible theft of cardholder data with respect to many of the U.S.-issued Alerted On Accounts that Visa found to be eligible for the ADCR process. For this reason as well, then, the Counterfeit Fraud Recovery Assessment violated the VIOR because even under a broad definition of the term "account compromise event" at least some of the U.S.-issued Alerted-On Accounts on which the assessment is based were ineligible for the ADCR process by reason of their not having suffered such an event.

Id.

Genesco next asserts that under the VIOR, the ADCR assessment process requires facts that Genesco violated PCI DSS and enabled the intruder(s) to enter Genesco's computer network and accomplish the theft or create the opportunity for theft. Id. at ¶ 55. Thus, Genesco contends that Visa's Counterfeit Fraud Recovery Assessments for these violations of Visa's VIOR lack factual proof of a PCI DSS violation by Genesco that could have allowed the theft of the full contents of any track on the magnetic stripe of that particular account.

According to Genesco, under Visa's VIOR, a group of Visa accounts can form the basis for a Visa acquirer's liability for Counterfeit Fraud Recovery under the ADCR process, but only where "incremental fraud" is attributable to that particular group of accounts. Id. at ¶ 56. Moreover, Genesco contends that under the VIOR, "incremental fraud" can properly be attributed to a particular group of Visa accounts only where that group of accounts incurred an amount of counterfeit fraud in excess of the amount of counterfeit fraud that normally would have been expected to have been reported on the accounts in question for the period in question. Id. Genesco's theory of recovery is that Visa did not show and could not reasonably conclude, for lack of proof, that the U.S.-issued Alerted-Accounts that Visa deemed eligible for the ADCR process suffered an amount of counterfeit

fraud in excess of the amount of counterfeit fraud that normally would have been expected to have been reported on that group of accounts for the period in question. Id. Thus, Genesco insists that Visa's Counterfeit Fraud Recovery Assessments also violated Visa's VIOR because the particular U.S.-issued Alerted-Accounts that Visa found eligible for the ADCR process, as a group, did not incur any amount of "incremental fraud" within the meaning of the VIOR. Id.

For the lack of factual predicates, Genesco also characterizes Visa's Counterfeit Fraud Recovery Assessments as unenforceable penalties because these assessments do not reflect actual damages to Visa. Id. at ¶ 57. Again, Genesco cites Visa's unlimited discretion to determine and impose these assessment as precluding any basis that these assessments are liquidated damages. Id. Moreover, Visa's U.S. issuers are neither parties nor third-party beneficiaries of the contracts between Wells Fargo and Fifth Third and Visa. Id. Thus, Genesco argues that neither Wells Fargo nor Fifth Third, as acquiring banks, can have any monetary exposure for damages suffered by Visa issuers.

c. Operating Expense Reimbursement Assessment

As to Visa's Operating Expense Recovery Assessments, Genesco contends that these assessments breached Visa's VIOR because Visa did not show that Genesco suffered an actual theft of cardholder data for all U.S.-issued Alerted-On Accounts that Visa deemed eligible for the ADCR process. Id. at ¶ 58. Genesco alleges that Visa did not demonstrate that Genesco committed a PCI DSS violation that allowed the theft of cardholder data for all U.S.-issued Alerted-Accounts that Visa considered eligible for the ADCR process. Id. Further, Genesco alleges that the U.S. Issuers' losses cited by Visa for incurred operating expenses for the U.S.-issued Alerted-On Accounts that Visa included in its ADCR process, were not shown to be the result of any theft tied to Genesco's

computer system. Id. According to Genesco, to impose assessments under Visa's VIOR for Operating Expense Recovery assessments, the Visa account must suffer an "account compromise event". Id. at ¶ 59. The ADCR allegedly defines an "account compromise event" as an actual theft of cardholder data relative to the account in question. Id. Further, according to Genesco, Visa did not show and could not reasonably conclude based upon forensic evidence that Genesco caused the theft of cardholder data or committed a PCI DSS violation that allowed the theft of cardholder data for all U.S.-issued Alerted-Accounts upon which Visa based its Operating Expense Reimbursement Assessments. Id. Again Genesco alleges that under its network, in the event of a cyber attack, the attack causes rebooting of the affected servers in Genesco's cardholder data environment, thereby eliminating any possible theft of cardholder data for many of the U.S.-issued Alerted-On Accounts that Visa considered eligible for Operating Expense Reimbursement Assessments.

For Visa's Operating Expense Recovery assessments, Visa allegedly did not show and could not reasonably conclude, for lack of proof, that any PCI DSS violation by Genesco enabled the cyber attackers to enter Genesco's computer network or obtain data necessary to steal payment card account data from Genesco's computer system. Id. at ¶ 61. Genesco contends that Visa's Operating Expense Recovery Assessments violated Visa's VIOR because Genesco could not have allowed the theft of the full contents of any track on the magnetic stripe of all U.S.-issued Alerted-On Accounts on which Visa based these assessment because Genesco did not commit a PCI DSS violation for such accounts.

Id.

Genesco's next claim is that Visa violated its VIOR that authorizes Operating Expense Recovery only when Visa's U.S. issuers incurred operating expenses for accounts as a result of an

account compromise event. Id. at ¶ 62. According to Genesco, Visa did not find and lacked any factual basis to find that Visa's U.S. issuers incurred any operating expenses for the U.S.-issued Alerted Accounts that Visa held eligible for these assessments. Id. Genesco again cites the lack of factual predicates to characterize these assessments as penalties, not damages. Genesco again reiterates that Visa's U.S. issuers are neither parties nor third-party beneficiaries of the contracts between the Acquiring Banks and Visa, so the Acquiring Banks cannot incur any breach-of-contract liability under those agreements for damages suffered by those issuers. Id.

Genesco's next claim is that in the DCRS Assessments, Visa violated its VIOR because Visa did not show and could not reasonably concluded that: (1) Genesco suffered a theft of cardholder data for all the non-U.S. issued Alerted-On Accounts that Visa found to be eligible for the DCRS process; (2) Genesco committed a PCI DSS violation that allowed the theft of cardholder data with respect to all the non-U.S. issued Alerted-On Accounts that Visa found to be eligible for the DCRS process; and/or (3) the non-U.S. issued Alerted-On Accounts that Visa found to be eligible for the DCRS process did not suffer an amount of counterfeit fraud in excess of the amount of counterfeit fraud that normally would have been expected to have been reported on that group of accounts for the period at issue. Id. at ¶ 64.

Visa allegedly compromised its DCRS process that is available for a "data compromise event" that means an actual theft of cardholder data relative to the account in question. Id. at ¶ 65. Genesco alleges Visa did not show and could not reasonably concluded that Genesco suffered a theft of cardholder data with respect to all the particular non-U.S. issued Alerted-Accounts that Visa found to be eligible for the DCRS assessments. Id. Visa allegedly found the Alerted-Accounts eligible without proof that those accounts had in fact been compromised during cyber attack on

Genesco's computer system. Id. For all other non-U.S. issued Alerted- Accounts that Visa found eligible, Genesco allege the lack of any forensic evidence that those accounts had been compromised during the cyber attacks on Genesco's computer system.

Genesco further alleges that under the VIOR a Visa account can be made eligible for the DCRS process only if the entity in question committed some violation of the PCI DSS that could have allowed the compromise (i.e., the theft) of the full contents of any track on the magnetic stripe of that particular account. Id. at ¶ 67. Visa allegedly did not show that Genesco committed a PCI DSS violation that allowed the theft of cardholder data with respect to all the non-U.S. issued Alerted-Accounts that Visa found to be eligible for the DCRS process. Id. In particular, Visa allegedly did not show and could not have reasonably concluded that any PCI DSS violation by Genesco enabled the cyber attackers to enter Genesco's computer network or enabled these attackers to steal payment card account data from Genesco's computer system. Id. Thus, the DCRS Assessments violated the DCRS because all of the non-U.S.-issued Alerted-On Accounts on which the assessment is based, were ineligible for the DCRS process due to the lack of a PCI DSS violation by Genesco that could have allowed the compromise of the full contents of any track on the magnetic stripe of a particular account. Id.

According to Genesco, under the DCRS a group of Visa accounts can form the basis for a Visa acquirer to be liable for the DCRS process only where "incremental fraud" is attributable to that particular group of accounts. Id. at ¶ 68. Moreover, under the DCRS "incremental fraud" can properly be attributed to a particular group of Visa accounts only where that group of accounts incurred an amount of counterfeit fraud in excess of the amount of counterfeit fraud that normally would have been expected to have been reported on the accounts in question for the period in

question. Id. Visa allegedly did not show that the non-U.S. issued Alerted-Accounts that Visa found to be eligible for the DCRS process incurred, as a group, involved an amount of counterfeit fraud in excess of the amount of counterfeit fraud that normally would have been expected to have been reported on that group of accounts for the period in question. Id. Genesco argues that the DCRS Assessments thus violated the DCRS because the particular non U.S. issued Alerted- Accounts that Visa found to be eligible for the DCRS process did not incur, as a group, any amount of "incremental fraud" within the meaning of the VIOR. Id.

Moreover, the DCRS Assessments are allegedly invalid to the extent these assessments included Alerted-Accounts issued by Visa Europe issuers. Id. at ¶ 69. The VIOR are explicit in stating that members of Visa Europe are separate from Visa, Inc. and therefore separately governed by the Operating Regulations of Visa Europe. Id. Thus, Genesco contends that neither the DCRS process nor VIOR, makes accounts issued by Visa Europe issuers eligible for the DCRS process. Id.

According to Genesco, the DCRS Assessment would be legally unenforceable even if it were valid under the VIOR, because the DCRS Assessments constitutes penalties- rather than damages- for the Acquiring Banks' allegedly having breached their contracts with Visa, and as such it is legally unenforceable under applicable law. Id. at ¶ 70. Further, Genesco asserts that Visa cannot show that the DCRS Assessments represent Visa's actual damages due alleged breaches by the Acquiring Banks' of their contractual obligation to cause Genesco to comply with the requirements of the PCI DSS. Id. Under Genesco's theory, by the terms of the DCRS, the DCRS Assessments cannot purports to constitute losses that Visa's non-US. issuers incurred by reason of the Acquiring Banks' alleged violations of their contractual obligation to Visa. Id. This alleged to be true because Visa's non-U.S. issuers are not parties to or third-party beneficiaries of the contracts between the Acquiring

Banks and Visa, so the Acquiring Banks could not have breached their contracts and caused any damages to those issuers. Assuming such liability, Gensco argues that the Acquiring Banks could not be liable as Visa issuers did not actually incur damages due to a data compromise event that results from a merchant's failure to be PCI DSS compliant. Id.

Thus, Genesco again reiterates that the DCRS's provisions are not valid as liquidated damages because: (1) DCRS liability is not intended to be compensatory damages for counterfeit fraud losses incurred by Visa due to a Visa acquirer's failure to ensure its merchants' PCI DSS compliance, but rather is to compensate such counterfeit fraud losses incurred by Visa's non-US issuers, who are not parties to or third-party beneficiaries of a Visa Acquirer Banks' contracts with Visa; (2) the VIOR purport to afford Visa unbounded discretion to determine the imposition and calculate the amounts of liability pursuant to the DCRS process; (3) the amount of any counterfeit fraud losses that Visa and/or its non-U.S. issuers may actually incur by reason of a Visa acquirer's failure to ensure its merchants' PCI DSS compliance is not only reasonably estimable, but calculable to the penny, to the extent they incur any such losses at all; and (4) DCRS liability is not Visa's exclusive damages remedy by reason of a Visa acquirer's failure to ensure its merchants' PCI DSS compliance. Id. Because the DCRS Assessment cannot be sustained as a valid award of either actual or liquidated damages by reason of the Acquiring Banks' alleged breaches of their contractual obligation to Visa to cause Genesco to comply with the PCI DSS, those assessments necessarily constitute penalties for such alleged breaches, and are unenforceable under applicable law regardless of whether such assessments are permitted by Visa's VIOR. Id.

B. Conclusions of Law

To survive a motion to dismiss, Genesco's complaint must "contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009)) (citation omitted). For such a motion, the Court must "'construe the complaint in the light most favorable to the plaintiff, accept all its allegations as true, and draw all reasonable inferences in favor of the plaintiff.'" In re Travel Agent Com'n Antitrust Litig., 583 F.3d 896, 903 (6th Cir. 2009) (citation omitted), but the Court "need not accept as true legal conclusions or unwarranted factual inferences . . . and conclusory allegations or legal conclusions masquerading as factual allegations will not suffice." (citations and quotation marks omitted).

In Iqbal, the Supreme Court explained the requirements for sustaining a motion to dismiss under Fed. Rule Civ. Proc. 12(b)(6):

Under Federal Rule of Civil Procedure 8(a)(2), a pleading must contain a "short and plain statement of the claim showing that the pleader is entitled to relief." As the Court held in Twombly, 550 U.S. 544 (2007), the pleading standard Rule 8 announces does not require "detailed factual allegations," but it demands more than an unadorned, the-defendant-unlawfully-harmed-me accusation. *Id.* at 555 (citing Papasan v. Allain, 478 U.S. 265, 286 (1986)). A pleading that offers "labels and conclusions" or "a formulaic recitation of the elements of a cause of action will not do." 550 U.S. at 555. Nor does a complaint suffice if it tenders "makes assertion[s]" devoid of "further factual enhancement." *Id.* at 557.

To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to "state a claim to relief that is plausible on its face." *Id.*, at 570. A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged. *Id.*, at 556. The plausibility standard is not akin to a "probability requirement," but it asks for more than a sheer possibility that a defendant has acted unlawfully. *Ibid.* Where a complaint pleads facts that are "merely consistent with" a defendant's liability, it "stops short of the line between possibility and plausibility of 'entitlement to relief.'" *Id.*, at 557 (brackets omitted).

Two working principles underlie our decision in Twombly. First, the tenet that a court must accept as true all of the allegations contained in a complaint is inapplicable to legal conclusions. Threadbare recitals of the elements of a cause of

action, supported by mere conclusory statements, do not suffice. *Id.* at 555. . . . Second, only a complaint that states a plausible claim for relief survives a motion to dismiss. *Id.* at 556. Determining whether a complaint states a plausible claim for relief will, as the Court of Appeals observed, be a context-specific task that requires the reviewing court to draw on its judicial experience and common sense. *Iqbal v. Hasty*, 490 F.3d 143, 157-58 (2d. Cir. 2007). But where the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged, but it has not "show[n]", "that the pleader is entitled to relief." Fed. Rule Civ. Proc. 8(a)(2).

In keeping with these principles a court considering a motion to dismiss can choose to begin by identifying pleadings that, because they are no more than conclusions, are not entitled to the assumption of truth. While legal conclusions can provide the framework of a complaint, they must be supported by factual allegations. When there are well-pleaded factual allegations, a court should assume their veracity and then determine whether they plausibly give rise to an entitlement of relief.

556 U.S. at 677-79.

In Blount Financial Services v. Walter E. Heller & Co., 819 F.2d 151, 153 (6th Cir. 1987), the Sixth Circuit explained that "Rule 9(b) requiring 'averments of fraud . . . with particularity' is designed to allow the District Court to distinguish valid from invalid claims in just such cases as this one and to terminate needless litigation early in the proceedings." (citation omitted). Rule 9(b) is also intended "to provide a defendant fair notice of the substance of a plaintiff's claim in order that the defendant may prepare a responsive pleading." American Town Ctr. v. Hall 83 Assocs., 912 F.2d 104, 109 (6th Cir. 1990). The Sixth Circuit ruled that the provisions of Fed. R. Civ. P. 8 and the requirement of Rule 9(b) are to be read in conjunction with each other. Michaels Bldg. Co. v. Ameritrust Co., N.A., 848 F.2d 674, 679 (6th Cir. 1988).

Under Ameritrust, the plaintiff can satisfy Rule 9(b)'s requirements by pleading the circumstances of the fraud, not the evidence. 848 F.2d at 680 n.9. Since Ameritrust, however, the Sixth Circuit reiterated the rule of this Circuit that FRCP 9(b) requires that fraud be pleaded with

particularity. To satisfy FRCP 9(b), a plaintiff must “at a minimum ‘**allege the time, place and contents of the misrepresentations upon which [the plaintiff] relied.**’” American Town Center, 912 F.2d at 109 (quoting Bender v. Southland Corporation, 749 F.2d 1205, 1216 (6th Cir. 1984)) (emphasis added).

On its face, Visa’s motion to dismiss challenges Genesco’s claims under California’s Unfair Competition Law (“UCL”)² and common law. Yet, these claims are premised upon Visa’s alleged breaches of its contracts with Fifth Third and Wells Fargo and Visa’s violations of the provisions of its VIOR. For these claims, Genesco essentially contends that Visa knew, or had reason to know, that its imposition and collection of Non-Compliance Fines and the Assessments from Fifth Third and Wells Fargo would be passed through to Genesco by those Banks. (Docket Entry No. 1, Complaint at ¶ 145). As to the substantive violations, Gensco asserts in sum that because Visa imposed these fines and assessments without factual justification, Visa engaged in an “unfair” business practice in violation of California’s UCL. Id. at ¶ 146. Because Visa allegedly misrepresented to the Banks that such fines and assessments were due in violation of Visa’s VIOR, Gensco asserts that Visa engaged in a “fraudulent” business practice. Id. at ¶ 147. Visa’s wrongful collection of \$13,298,900.16 in these fines and assessments is further alleged to be an “unlawful, unfair and fraudulent business practices” prohibited by the UCL for which Genesco seeks restitution, as the party injured in fact. Id. at ¶ 148. In its Seventh claim, Genesco reasserts its factual allegations about Visa’s imposition and collection of these fines and assessments for Visa’s unjust enrichment at Gensco’s expense for which Genesco also seeks restitution and damages. Id. at ¶¶ 151-56.

California’s UCL prohibits five different types of wrongful conduct: (1) an “unlawful . . .

² The Visa Defendants’ principal offices are in California.

business act or practice”; (2) an “unfair . . . business act or practice”; (3) a “fraudulent business act or practice”; (4) “unfair, deceptive, or untrue or misleading advertising”; and (5) “any act prohibited by [California’s Business and Professional Code].” Cal. Bus. & Prof. Code §§ 17500-17577.5, § 17200. UCL’s substantive standards are disjunctive because “unlawful” business practices are forbidden under the UCL even if the practices are not “unfair” or “fraudulent”. See Cel-Tech Communications, Inc. v. L.A. Cellular Tel. Co., 20 Cal.4th 163, 180 (Cal. 1999). Under California UCL,

[S]ection 17200 is not confined to anti-competitive business practice but is equally directed toward “the right of the public to protection from fraud and deceit.” Furthermore, the section 17200 proscription of “unfair competition is not restricted to deceptive or fraudulent conduct but extends to any unlawful business practice. The Legislature apparently intended to permit courts to enjoin ongoing wrongful business conduct in whatever context such activity might occur.

Committee on Children's Television, Inc. V. General Foods Corp., 35 Cal.3d 197, 209–10 (1983), superseded by statute, Cal. Bus. & Prof. Code § 17204, on other grounds (internal quotations and citations omitted). “It is not necessary that the predicate law provide for private civil enforcement.” Saunders v. Superior Court, 27 Cal. App. 4th 832, 839 (Cal. Ct. App. 1994). A direct relationship with the defendant is not necessary for a UCL claim so long as the Plaintiff suffered an injury or loss of funds due to the Defendant’s practice. See Law Office of Matthew Higbee v. Expungement Assistance Servs., 214 Cal. App. 4th 544, 563 (Cal. Ct. App. 2013).

As to the scope of California’s UCL, the California Supreme Court stated that

[Section 17200] defines ‘unfair competition to include any unlawful, unfair or fraudulent business act or practice. . . . Its coverage is sweeping, embracing anything that can properly be called a business practice and that at the same time is forbidden by law.... By proscribing any unlawful business practice, section 17200 borrows violations of other laws and treats them as unlawful practices that the unfair competition law makes independently actionable. ... However, the law does more

than just borrow. The statutory language referring to any unlawful, unfair or fraudulent practice ... makes clear that a practice may be deemed unfair even if not specifically proscribed by some other law. Because Business and Professions Code section 17200 is written in the disjunctive, it establishes three varieties of unfair competition-acts or practices which are unlawful, or unfair, or fraudulent.

Cel-Tech Comms, 20 Cal. 4th at 180 (internal quotations omitted). “The statute is intentionally broad to give the court maximum discretion to control whatever new schemes may be contrived, even though they are not yet forbidden by law.” People ex rel. Renne v. Servantes, 86 Cal. App. 4th 1081, 1095 (Cal. Ct. App. 2001).

“Whether a practice is deceptive or fraudulent ‘cannot be mechanistically determined under the relatively rigid legal rules applicable to the sustaining or overruling of a demurrer.’ Rather, the determination is one question of fact, requiring consideration and weighing of evidence from both sides before it can be resolved.” McKell v. Washington Mut., Inc., 142 Cal. App. 4th 1457, 1472, (Cal. Ct. App. 2006) (internal citations omitted). California courts consider “[w]hether a business act or practice constitutes unfair competition with Section 17200 [is] a question of fact.” Watson Labs, Inc. v. Rhone-Poulenc Rorer, Inc., 178 F. Supp.2d 1099, 1117 (C.D. Cal. 2001). To extent that injunctive relief is sought, Plaintiff must also allege actual injury. Cal. Bus & Prof. Code §§ 17204, 17535.

An “unlawful” act under California’s UCL is defined broadly as a business act or practice that is prohibited by a law. Cel-Tech Comms, 20 Cal.4th at 180. “[S]ection 17200 ‘borrows’ violations of other laws and treats them as unlawful practices that the unfair competition law makes independently actionable.” Id. A “fraudulent” practice is defined more broadly than common law fraud and only requires allegations that “members of the public are likely to be deceived.” Express, LLC v. Fetish Group, Inc., 464 F.Supp.2d 965, 980 (C.D. Cal. 2006) (quoting Olsen v. Breeze, Inc.,

48 Cal.App.4th 608, 617-18 (1996)).

For “unfair” business acts or practices, “California's unfair competition law prohibits not only unlawful business practices but also unfair business practices. A business practice that is not unlawful may nonetheless be actionable as an ‘unfair’ business practice. An unfair business practice under the UCL is ‘one that either offends an established public policy or is immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers’.” McDonald v. Coldwell Banker, 543 F.3d 498, 506 (9th Cir. 2008) (internal quotations omitted). The “test . . . is that a practice merely be unfair.” Allied Grape Growers v. Bronco Wine Co., 203 Cal. App. 3d 432, 452 (Cal. Ct. App. 1988). This requires that the court balance the “the impact of the practice or act on its victim . . . against the reasons, justifications and motives of the alleged wrongdoer.” Klein v. Earth Elements, Inc., 59 Cal. App. 4th 965, 969 (Cal. Ct. App. 1997). The “test for determining an ‘unfair’ practice is [whether] the gravity of the harm to the victim outweighs the utility of the defendant's conduct.” Servantes, 86 Cal. App. 4th at 1095; see also Scripps Clinic v. Super. Ct., 108 Cal.App.4th 917, 940 (Cal. Ct. App. 2003). Yet, “[c]ourts may not simply impose their own notions of the day as to what is fair or unfair.” Cel-Tech Comms, 20 Cal 4th at 182; see also Bias v. Wells Fargo & Co., 2013 WL 1787158, (N.D. Cal. April 25, 2013) (explaining UCL’s three tests for unfairness “in the consumer context.”).

Here, Genesco’s UCL claims are tied to Visa’s contracts with Fifth Third and Wells Fargo. Defendants argue that Genesco’s contract based claims do not state viable UCL claims, citing Linear Tech Corp. v. Applied Materials Inc., 152 Cal. App. 4th 115 (2007). Id. at 135. (“[W]here a UCL action is based on contracts not involving either the public in general or individual consumers who are parties to the contract, a corporate plaintiff may not rely on the UCL for the relief it seeks.”); see

also Graphic Pallet & Transport Inc. v. Balboa Capital Corp., 11-9101, 2012 WL 195 2745 at *6 (N.D. Ill. May 30, 2012) (“California courts have refused to allow commercial parties to use § 17200 to resolve disputes over their economic relationships.”); see also Korea Supply Co. V. Lockheed Martin Inc., 29 Cal. 4th 1134, 1150 (2003) (the UCL “is not an all-purpose substitute for a tort or contract action.”), Dollar Tree Stores Inc. V. Topmaya Partners L.L.C., 875 F. Supp2d 1058, 1083 (N.D. Cal. 2012) (“a breach of contract . . . does not implicate the public in general or individual consumers.”). Linear Technology was a patent infringement action with related claims of breach of contract and good faith and fair dealing where the California appellate court affirmed the dismissal of a UCL claim arising out of that dispute:

In this case, however, the superior court properly dismissed this cause of action on demurrer for reasons independent of the evidence that may be presented. The UCL was enacted “to protect both consumers and competitors by promoting fair competition in commercial markets for goods and services.” (Kasky v. Nike, Inc., supra, 27 Cal.4th at p. 949, 119 Cal.Rptr.2d 296, 45 P.3d 243; see also Paulus v. Bob Lynch Ford, Inc., supra, 139 Cal.App.4th at p. 676, 43 Cal.Rptr.3d 148.) Here, the alleged victims are neither competitors nor powerless, unwary consumers, but Linear and other corporate customers in Silicon Valley, “each of which presumably has the resources to seek damages or other relief ... should it choose to do so.” (Rosenbluth International, Inc. v. Superior Court (2002) 101 Cal.App.4th 1073, 1078, 124 Cal.Rptr.2d 844.) And the source of the fraudulent and unfair practices is the misrepresentation made in purchase orders between respondent sellers and Linear, in which each seller warranted that no infringement claim would result from Linear's use of that seller's equipment. Thus, contrary to Linear's representation, the harm it suffered did result from contracts specifically with the plaintiff. The other alleged victims likewise are sophisticated corporate customers who have entered or will enter their own contracts with respondents, although neither these victims nor the contracts are identified in the complaint. In these circumstances, where a UCL action is based on contracts not involving either the public in general or individual consumers who are parties to the contract, a corporate plaintiff may not rely on the UCL for the relief it seeks. (Id. at pp. 1077–1079, 124 Cal.Rptr.2d 844.) “By purporting to act as their self-appointed representative and asserting claims on their behalf in a UCL action, [Linear] could in fact deprive [respondents'] alleged victims of the individual opportunity to seek remedies far more extensive than those available under the UCL.” (Id. at p. 1079, 124 Cal.Rptr.2d 844.) Thus, to the extent that Linear purports

to represent other customers, permitting its UCL claim would raise “ ‘serious fundamental due process considerations.’ ” (Ibid., quoting *Bronco Wine Co. v. Frank A. Logoluso Farms* (1989) 214 Cal.App.3d 699, 720, 262 Cal.Rptr. 899.) The Rosenbluth court did not limit its holding to allegations of fraudulent conduct. Accordingly, notwithstanding the wide range of conduct that can be deemed “unfair” within the meaning of section 17200, the reasoning of Rosenbluth is equally fitting in cases involving allegations of unfairness under the UCL. The superior court properly sustained respondents’ demurrers to the claim of unfair competition for failure to state a viable cause of action.

152 Cal App. 4th at 135.

In opposition, Genesco cites California decisions that recognize claims related to contracts to be actionable under the UCL. “An act that breaches a contract may also breach the UCL . . . when the act is unfair, unlawful or fraudulent for some additional reason.” James v. UMG Recordings, Nos. C 11-1613 SI, C 11-2431 SI, 2011 WL 5192476 at *5 (N.D. Cal. Nov. 1, 2011) (quoting Boland, Inc. v. Rolf C. Hagen (USA) Corp., 685 F. Supp. 2d 1094, 1110 (E.D. Cal. 2010)); Comercializadora Recmaq Limitada v. Hollywood Auto Mall, LLC., No. 12cv0945, 2013 WL 2248140 at *6, 10, 11 (S.D. Cal. May 20, 2013) (complaint alleging breach of purported oral contract for agent to purchase heavy machinery and misrepresentations about the funds use were held to state fraudulent and unfair acts and practices under UCL); Clayworth v. Pfizer, 49 Cal. 4th 758, 789 (Cal. 2011) (valid UCL claim against pharmaceutical manufacturers and distributors for charging an artificially inflated price under their contracts with pharmacies); and Allied Grape Growers v. Bronco Wine Co., 203 Cal. App. 3d 432, 452-53 (Cal. Ct. App. 1998) (affirmed a jury verdict awarding damages to a grape growers co-op under a contract). Genesco argues that California courts dismiss UCL claims based on a breach of contract, where “additional reason” did not exist to find those breaches of contract to be unlawful, unfair, or fraudulent.

The Court agrees with the California district court that observed that: “a breach of contract may form the predicate for a section 17200 claim, **provided it also constitutes conduct that is unlawful, or unfair, or fraudulent.**” Nat’l Rural Telecomm. Co-op., 319 F. Supp. 2d 1059, 1074 (internal quotation and citation omitted, emphasis added). Although “Section 17200 does not give courts carte blanche to evaluate the fairness of the contract,” an unfair business practice claim based upon “monies withheld in accordance with a contractual provision that is either missing or allegedly unenforceable due to the unconscionable nature in which it was imposed,” sufficiently alleges an unfair business practice claim. Roling v. E*Trade Securities, LLC, 756 F. Supp. 2d 1179, 1193 (N.D. Cal. 2010); see also Stop Youth Addictions, Inc. V. Lucky Stores Inc. 17 Cal. 4th 553, 558 (1998) (cognizable claim under the UCL, a controversy between for profits corporations in dispute over retail sales to minors), superseded by statute, Cal. Bus. & Prof. Code § 17204, on other grounds.

Contracts with express provisions may be challenged as unconscionable under the UCL. Armendariz v. Foundation Health Psychcare Services, Inc., 24 Cal.4th 83, 114 (Cal. 2000). Unconscionability has procedural and substantive requirements under California law. The procedural requirement focuses on contract negotiation and formation for oppression or surprise due to unequal bargaining power. Id. The substantive element of unconscionability involves the fairness of an agreement's actual terms and assessment of whether those provisions are overly harsh or one-sided. Id. The UCL has been applied to banking lending agreements. Hood v. Santa Barbara Bank of Trust, 143 Cal. App. 4th 526 (Cal. Ct. App. 2006). Thus, where express commercial contract provision implicates the public interest or violates public policy or law or poses harm to consumers or competitors in the marketplace, such contracts can state a claim under California’s UCL.

Visa's principal argument is that the express terms of its contracts with Wells Fargo and Fifth Third that are the heart of this controversy, preclude any claim under California's UCL or basis for Genesco's unjust enrichment claim. Yet, in support of its motion, Visa observes that Genesco's breach of contract claims possess "factual and legal flaws." (Docket Entry No. 31, Visa Memorandum at 2). If true, and so determined in subsequent proceedings, then there is not any breach of contract so as to bar Genesco's UCL and common law claims. Federal Rule of Civil Procedure 8(d)(2) permits the pleading of alternative and inconsistent theories of recovery. Genesco's pleadings reflects a permissible form of alternative pleading by asserting different legal grounds or theories for relief, in the event Genesco does not prevail on its breach of contract claims.

Moreover, the factual allegations here involve more than the parties, Fifth Third and Wells Fargo. With their indemnification agreements with Genesco and their agreements with Visa, Fifth Third and Wells Fargo enabled Visa to determine and impose unilaterally more than \$13 million in fines and assessments allegedly without a demonstrated factual basis for doing so. According to Genesco's complaint, Visa's assessments were not based on forensic data and allegedly the forensic data affirmatively showed that not all Visa accounts in Visa's assessment were compromised. Genesco alleges that Visa permits the unencrypted data on its "mag-stripe-swipe" transactions that enabled a cyber attack and caused the assessments and fines. These factual allegations create a controversy that allegedly impacts the operation of the Visa card payment system and implicates consumers, merchants and other banks impacted by the cyber attack on Genesco's computer network. Visa's contracts and VIOR create a structure or "environment" that could be found to be harmful to competition at the merchant level and establish unfairness in the market for credit and

debit card transactions of which merchants and consumers are key players.³ California's UCL extends to controversies that involve commercial entities, including actions for recovery of funds not paid directly to the defendant, but fairly traceable to the Defendant as the source of Plaintiff's losses in the controversy. Although Visa contends its contractual provisions at issue are necessary for the efficient operation of its card payment system, Genesco alleges violations by Visa of its own standards and procedures for imposing such fines and assessments. To the extent that Visa's contracts effectively permit fines and assessments upon banks and merchants without factual predicates, the imposition of these fines and assessment could be found to be an unfair and unlawful business practice.

Moreover, Genesco asserts that these fines and assessments are also penalties that are unenforceable under California law. Under California law, penalties were held unenforceable as a matter of law where a commercial contract sets the same fixed sums for various types of breaches of the contract for delivery of good under a contract. In Dollar Trees Stores Inc. V. Toyama Partners, L.L.C., 875 F. Supp. 2d 1058 (N.D. Cal. 2012), that Court found an unenforceable penalty in what appear to be comparable circumstances.

Toyama argues that the liquidated damages provision is unenforceable for the additional and independent reason that it imposes a \$2,500 per day charge until all

³See In re Visa Check/Mastermoney Antitrust Litigation No. 96-CV-5238, 2003 WL 1712568 (E. D. N.Y. April 1, 2003) (denying motion for summary judgment on merchants' claims for Visa's illegal tying arrangements and excessive fees); United States v. Visa U.S.A. Inc., 163 F. Supp.2d 322, (E. D. N. Y. 2001) aff'd, 344 F.3d 229 (2d Cir. 2003) (Sotomayor, J) (Visa's exclusionary rules imposed due to its market power was an unreasonable restraint of trade). These decisions cited proof of Visa's monopoly power in the debit card market. Consumers alleged injuries from those practices in higher retail prices. Bennett v. Wal-Mart Stores, Inc. No. 06-CV-5304, 2011 WL 3878330 (E. D. N. Y. Sept. 02, 2011).

of the Delivery Conditions are met, which is in perpetuity if all of the Delivery Conditions are not met. The provision states that liquidated damages shall accrue “for each day or part thereof which elapses between the Anticipated Delivery Date . . . and the date when all of the Delivery Conditions shall have been satisfied by Landlord.” ARL § D.1.c.1. The ARL defines the “Term of this Lease” as follows:

The Original Lease Term (“Original Lease Term”) shall commence upon the Lease Term Commencement Date and, subject to C.1, shall expire on the last day of the one hundred thirty-second (132nd) full month following the Lease Term Commencement Date (“Lease Expiration Date”), unless sooner terminated in accordance with the terms of this Lease. Tenant shall have the right and option to extend the term of this Lease for one (1) additional period of six (6) years (such period referred to the “Renewal Term”) in accordance with Section C.3.

Each of the Original Lease Term [and] the Renewal Term, if so exercised, shall be individually deemed a “Lease Term” for the purposes of this Lease.

ARL § A.8. The ARL provides that the “Lease Term Commencement Date” “shall commence the earlier of (a) ninety (90) days after the Turnover Date or (b) when Tenant opens for business in the Premises.” ARL § A.6. Toyama argues that the 17 year lease term does not commence until 90 days after the premises is turned over to Dollar Tree or it opens for business, and thus that under the plain language of the ARL, liquidated damages accrue indefinitely if the delivery conditions are never satisfied.

Dollar Tree's opposition does not address this argument, and asserts without analysis that the period of recovery is limited to 17 years, the maximum term of the lease. However, Dollar Tree does not cite any language in the ARL for this assertion. The Court agrees with Toyama that under the plain language of the ARL, the term of the lease does not commence until 90 days after the date on which the “Premises are actually delivered to Tenant in accordance with the terms of this Lease,” and that the store shall not be deemed to be delivered until satisfaction of all the Delivery Conditions. Thus, the term of the lease begins after compliance with the Delivery Conditions. The term of the lease is not the period governing the assessment of liquidated damages. Instead, under Section D.C.1, liquidated damages begin to accrue as of June 15, 2009, at a rate of \$2,500 per day if the delivery conditions had not been satisfied by June 25, 2009, and they continue to accrue until all of the delivery conditions are met; if the delivery conditions are never met, liquidated damages accrue indefinitely.

The Court concludes that Toyama has met its burden to show that the liquidated damages provision is unenforceable because it imposes the same \$2,500 penalty for at least nine different types of breach of varying degrees of

magnitude, and because it imposes that penalty indefinitely until Toyama satisfies all of the Delivery Conditions. By imposing potentially unlimited damages, the liquidated damages provision bears no rational relationship to the actual damages that could be expected to flow from the different types of breaches. Because the Court reaches this conclusion as a matter of contract interpretation, the Court does not reach the parties' arguments about whether Dollar Tree intended the liquidated damages to act as a penalty, or whether the amount of liquidated damages was based on any financial or damage analysis. Even if, as Dollar Tree asserts and Toyama disputes, Dollar Tree arrived at the \$2,500 daily damages based upon an analysis of its lost profits and loss of goodwill in the event that it was unable to open its store, the provision is still unreasonable because under the plain language of the ARL, Dollar Tree is entitled to \$2,500 per day beginning June 15, 2009, in perpetuity until Toyama satisfies all of the Delivery Conditions.

Id. at 1072-73 (emphasis added and footnote omitted).

Genesco's allegations are that Visa imposed these fines and assessments without factual support and contrary to forensic evidence that not all U. S. Visa Alert Accounts were harmed by the cyber attack on Genesco's computer system. Given Genesco allegations, if Visa's contracts impose assessments based upon possible risk of injuries in the event of a breach of a cardholder's data, without an actual theft of such data, then that assessment may be an unenforceable penalty under California law. The Court concludes that Genesco's complaint alleges sufficient facts to support a claim that Visa's fines and assessments are penalties. Thus, the Court concludes that Genesco's complaint states viable and plausible UCL and common law claims under California law for which restitution, as the actual payer of these assessments and fines, is a viable remedy under California law. In Bank of the West v. Superior Court, 2 Cal.4th 1254 (Cal. 1992), where plaintiff sought disgorgement, the UCL was deemed to authorize restitution of any money which a trial court finds was acquired by any illegal practice. Id. at 1267. A court may order restitution without individualized proof of deception, reliance and injury, if the particular practice is "unfair" to

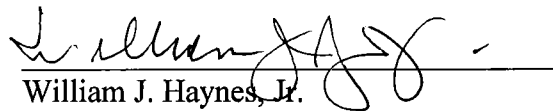
consumers. Davis v. Ford Motor Credit Co., 179 Cal. App. 4th 581, 594–98 (Cal. Ct. App. 2009); Harmon v. Hilton Group, No. C–11–03677 JCS, 2011 WL 5914004, at *8 (N.D. Cal. Nov.28, 2011).

Thus, the Court concludes that Genesco's complaint states viable claims under California law.⁴

For these reasons, the Court concludes that the Visa Defendants' motion to dismiss Genesco's sixth and seventh claims should be denied.

An appropriate Order is filed herewith.

Entered this the 18th day of July, 2013


William J. Haynes, Jr.
Chief United States District Judge

⁴ This District has recognized common law claims under Tennessee law against a credit card company and a merchant concluding that those entities owe legal duties to each other and a cardholder in transactions in the credit card system. See Permobil Inc. v. American Express Travel Related Services Co. Inc., 571 F. Supp2d 825, 836-45 (M. D. Tenn. 2008) (credit card issuers) (Trauger, J.) and Permobil Inc. v. GMRI, Inc., No. 3:09cv1145, 2011 WL 441397 (M. D. Tenn. Feb. 8, 2011) (merchant liability) (Haynes, J.)